DECEMBER 2020

MIDLAND HEALTH
Compliance Hotline
877•780•9367

COMPLIANCE CONNECTION

This newsletter is prepared by the Midland Health Compliance Department and is intended to provide relevant HIPAA privacy issues and hot topics.

IN THIS ISSUE

HIPAA Privacy Rule: Myths & Facts

Myth: ***Patients Can Sue Healthcare Providers for Violating HIPAA***

Power to the people! You break the law, and you get sued. It's common sense. Common folks need to have the ability to sue healthcare providers for not complying with HIPAA regulations, right?

Fact: Even in case of a violation of the HIPAA Privacy Rule, patients cannot sue healthcare providers.

It's all about steady justice. If a healthcare provider fails to comply with HIPAA privacy regulations, you must file a written complaint. If there are reasonable grounds to investigate the complaint, the Secretary of Health and Human Services may do so at its own discretion.

Best case scenario, there may be some civil penalties and criminal sanctions imposed on said healthcare provider. But you as a patient don't have as much say as you might've hoped.

Resource:
https://www.qminder.com/hipaa-myths-debunked/

HIPAA and the Holidays

As the holiday season builds momentum we are faced with numerous distractions like holiday decorations, taking advantage of online sales and soaking in the traditions that we look forward to each year. But this season of joy and giving should also be met with a heightened sense of awareness and adherence to HIPAA policies and procedures.

You're likely thinking to yourself, "How can Christmas, Hanukkah, Kwanza or the New Year impact HIPAA?" Well, those holidays can't, but your employees' behavior sure can.

Electronic Protected Health Information (ePHI): *This busy season will cause some employees to take advantage of online shopping while at work. While that seems relatively harmless, and in most cases it is, this also invites the possibility of introducing viruses into your system from unprotected and/or unapproved sites.*

Physical Security: *Unfortunately, the season of "giving" for some means a season of "taking" for others. Generally, criminal activity like property theft and break-ins rise during the shopping season. This makes it extremely important for your entity to adhere to mandatory HIPAA Physical Safeguards. Specifically, entities are required to "implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft." [The HIPAA Security Rule: § 164.310(a)(2)(ii)]*

Workstation Security: *While employees struggle to keep up with the demand, they are more likely to be careless about workstation security. They become less likely to lock their computers when they walk away from their station. While these activities seem relatively harmless, these are violations that can cost the entity greatly if it leads to breaches of PHI or ePHI.*

Visitors and Guests: *The holidays aren't nearly as fun without office holiday parties. These parties generally include catered meals, outside delivery services and even invited guests. Entities should ensure that they have a documented visitor/guest policy and procedure and that their employees follow that procedure.*

Tone of Voice: *One of the biggest complaints that our office receives regarding patient privacy is the tone of voice used by employees and staff as they discuss their health conditions. Staff should be advised of this concern and reminded of the importance of using a professional tone that would not give rise to unauthorized or inappropriate disclosures of PHI.*

This is without argument "the most wonderful time of the year." It's a time to enjoy family, get reacquainted with friends, and provide for the health and well-being of patients. As the activity of the season builds, it is important to make every effort to ensure that your entity is in compliance with HIPAA regulations. Adhering to appropriate policies and procedures will not only ensure that you provide appropriate patient care, it will also reduce the likelihood of liability for violations which is a great way to start the New Year.

Resource: *https://alabamamedicine.org/hipaa-and-the-holidays/*

DID YOU KNOW...

HIPAA Violation...

Emailing ePHI to Personal Email Address Accounts and Removing PHI from Hospital Facility

Regardless of the intentions, whether it is to get help with spreadsheets, complete work at home to get ahead for the next day, or to catch up on a backlog, it is a violation of HIPAA Rules. Further, any emailing of ePHI to a personal email account could be considered theft, the repercussions of which could be far more severe than termination of an employment contract.

Resource: https://www.hipaajournal.com/common-hipaa-violations/

MIDLAND HEALTH

NEWS

Office 365 Users Targeted in Microsoft Teams Phishing Scam

A new Office 365 phishing campaign has been detected by researchers at Abnormal Security that spoofs Microsoft Teams to trick users into visiting a malicious website hosting a phishing form that harvests Office 365 credentials.

Microsoft Teams has been adopted by many organizations to allow remote workers to maintain contact with the office. In healthcare the platform is being used to provide telehealth services to help reduce the numbers of patients visiting healthcare facilities to control the spread of COVID-19.

Microsoft reported in a June call announcing financial earnings for the quarter ended June 30, 2020 that Microsoft Teams is now used by more than 150 million students and teachers. Over 1,800 different organizations have more than 10,000 Teams users, and 69 organizations have over 100,000 Teams users. The use of Microsoft Teams in healthcare has also been growing, with 46 million Teams meetings now being conducted for telehealth purposes. The increase in usage due to the pandemic has presented an opportunity for cybercriminals.

According to figures from Abnormal Security, the latest campaign has seen the fake Microsoft Teams emails sent 50,000-plus Office 365 users so far. The messages appear to be sent from a user with the display name "There's new activity in Teams," making the messages appear to be automated notifications from Teams.

The messages advise users to log into Teams as the community is trying to get in touch. The emails include a button to click to login to Teams that has the display text – "Reply in Teams." The messages include a realistic looking footer with the Microsoft logo and options to install Microsoft Teams on iOS and Android.

The links in the email direct the user to a Microsoft login page that is a carbon copy of the official login prompt, aside from the domain on which the page is hosted. That domain starts with "microsftteams" to make it appear genuine.

Read entire article:
https://www.hipaajournal.com/office-365-users-targeted-in-microsoft-teams-phishing-scam/

NEWS

Hospital Ransomware Attack Results in Patient Death

Ransomware attacks on hospitals pose a risk to patient safety. File encryption results in essential systems crashing, communication systems taken out of action, and clinicians prevented from accessing patients' medical records.

Highly disruptive attacks may force hospitals to redirect patients to alternate facilities, which recently happened in a ransomware attack on the University Clinic in Düsseldorf, Germany. One patient who required emergency medical treatment for a life threatening condition had to be rerouted to an alternate facility in Wuppertal, approximately 21 miles away. The redirection resulted in a one-hour delay in receiving treatment and the patient later died. The death could have been prevented had treatment been provided sooner.

The attack occurred on September 10, 2020 and completely crippled the clinic's systems. Investigators determined that the attackers exploited a vulnerability in "widely used commercial add-on software" to gain access to the network. As the encryption process ran, hospital systems started to crash and medical records could not be accessed.

The medical clinic was forced to de-register from emergency care, postpone appointments and outpatient care, and all patients were advised not to visit the medical clinic until the attack was remediated. A week later normal function at the hospital has still not resumed, although the hospital is now starting to resume essential systems.

According to a recent Associated Press report, 30 servers at the hospital were affected. A ransom demand was found on one of the encrypted servers. The hospital alerted law enforcement which made contact with the attackers using the information in the ransom note.

Read entire article:
https://www.hipaajournal.com/hospital-ransomware-attack-results-in-patient-death/

HIPAAQuiz

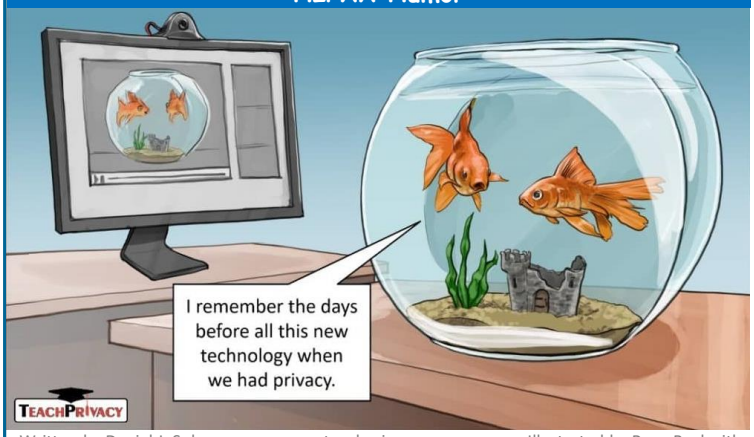
Which of the following is NOT an example of PHI?

a. Patient's demographic information in computer for appointment at health department
b. Patient's paper lab report that hasn't been filed yet
c. A report containing the number of HIV cases in the state of TN
d. A nurse discussing a patient's diagnosis with a physician

Answer: c

U.S. Department of Health and Human Services defines Protected Health Information (PHI) as individually identifiable information that falls into 18 types of identifiers (e.g., name, photo, phone number, email address, SS#, etc.). A report containing the number of cases is not an example of PHI because "identifiers" are not included.

HIPAA Humor



Written by Daniel J. Solove www.teachprivacy.com Illustrated by Ryan Beckwith

IN OTHER COMPLIANCE NEWS

LINK 1

September 2020 Healthcare Data Breach Report: 9.7 Million Records Compromised

https://www.hipaajournal.com/september-2020-healthcare-data-breach-report-9-7-million-records-compromised/

LINK 2

Exposed Broadvoice Databases Contained 350 Million Records, Including Health Data

https://www.hipaajournal.com/exposed-broadvoice-databases-contained-350-million-records-including-health-data/

LINK 3

Dickinson County Health Suffers Ransomware Attack

https://www.hipaajournal.com/dickinson-county-health-suffers-ransomware-attack/

LINK 4

Piedmont Cancer Institute Phishing Attack Impacts 5,000 Patients

https://www.hipaajournal.com/piedmont-cancer-institute-phishing-attack-impacts-5000-patients/

THUMBS UP to all MH Departments for implementing awareness of...

MIDLAND HEALTH

- *Main Campus*
- *West Campus*
- *Legends Park*
- *501a Locations*